J. Empir. Soc. Sci. Stud. 7(1)

Psychological Effects of Cybercrime on Minorities: Short-Term and Long-Term Impacts

Jonathan Rhoads

Mount Allison University, Sackville, New Brunswick

Abstract

Objective: The objective of this study was to examine the psychological effects of cybercrime on individuals who belong to minority groups.

Method: This study utilized a literature review approach to analyze previous research on the topic. A range of databases were searched, including PubMed and PsycINFO.

Results: The findings of this study indicated that cybercrime can have both short-term and long-term psychological effects on individuals who belong to minority groups. The short-term effects include fear and anxiety, loss of trust, and post-traumatic stress disorder (PTSD). Long-term effects include chronic stress, depression and anxiety, social isolation, and financial impacts.

Conclusion: This study highlights the importance of addressing the psychological effects of cybercrime on minorities through supportive services such as counseling, therapy, and community support. Additionally, measures should be taken to prevent cybercrime and provide justice to victims. It is crucial to recognize the impact of cybercrime on minority individuals and provide adequate support to mitigate the psychological effects.

Introduction

Cybercrimes, also known as computer crimes, are criminal activities that are committed using computers or the internet. These types of crimes have become increasingly prevalent in recent years, due to the rise of technology and the widespread use of the internet. Cybercrimes can range from relatively minor offenses, such as hacking into someone's social media account, to major crimes, such as stealing sensitive information from large corporations or governments.

One of the most common types of cybercrime is hacking. Hacking involves gaining unauthorized access to a computer system or network. This can be done for a variety of reasons, including theft of sensitive data, sabotage, or simply for the challenge of breaking into a secure system. Hackers use a variety of techniques to gain access, including phishing scams, malware, and brute force attacks.

Another type of cybercrime is identity theft. Identity theft occurs when someone steals personal information, such as a social security number or credit card information, and uses it for fraudulent purposes. This can include opening credit accounts, taking out loans, or even committing crimes in the victim's name. Identity theft is a serious crime that can cause significant financial and emotional harm to the victim.

Cyberstalking is another type of cybercrime that has become increasingly prevalent in recent years. Cyberstalking involves using the internet or other electronic means to harass, intimidate, or threaten someone. This can include sending unwanted messages, posting inappropriate content online, or even tracking someone's movements using GPS technology. Cyberstalking can be particularly frightening, as it can be difficult to escape from the harassment and the perpetrator can remain anonymous.

Phishing is another common type of cybercrime. Phishing involves tricking people into revealing their personal information, such as passwords or credit card numbers, by posing as a legitimate business or organization. Phishing scams can be carried out through email, social media, or even text messages. These scams can be difficult to spot, as they often appear to be from a legitimate source.

Malware is a type of software that is designed to harm or disrupt computer systems. Malware can take many forms, including viruses, Trojans, and worms. These types of programs can be used to steal data, spy on users, or even take control of a

computer system. Malware can be particularly dangerous because it can spread rapidly and infect multiple systems.

Distributed denial of service (DDoS) attacks are another type of cybercrime. DDoS attacks involve overwhelming a website or computer system with traffic, effectively shutting it down. These attacks can be carried out by individuals or groups, and can be used for a variety of reasons, including political activism or extortion.

Ransomware is a type of malware that is designed to encrypt a user's files and demand payment in exchange for the decryption key. Ransomware attacks can be particularly devastating, as they can result in the loss of important data or even the complete shutdown of a computer system. These attacks can be carried out through email, social media, or even infected websites.

Cyberbullying is another type of cybercrime that is becoming increasingly prevalent, particularly among young people. Cyberbullying involves using the internet or other electronic means to harass, intimidate, or embarrass someone. This can include posting inappropriate content online, sending threatening messages, or even creating fake profiles to impersonate someone else. Cyberbullying can be particularly harmful, as it can be difficult for victims to escape the harassment and the perpetrator can remain anonymous.

Cybercrimes can have a disproportionate impact on minority communities, including racial and ethnic minorities, LGBTQ+ individuals, and people with disabilities. These groups may be more likely to experience harassment, bullying, or discrimination online, and may also be more vulnerable to certain types of cybercrime, such as identity theft or online fraud.

For example, individuals from minority communities may be more likely to experience phishing scams that target them with fraudulent emails or social media messages. These scams may use language or images that are specific to their cultural background or community, making them more likely to fall for the scam. Similarly, members of minority communities may be more likely to be targeted by online harassment or bullying, which can have a significant impact on their mental health and well-being.

In addition, some cybercrimes may specifically target members of minority communities. For example, identity theft may be used to target individuals who belong to a particular racial or ethnic group, which can have a significant impact on their financial and personal well-being. Similarly, hate crimes and hate speech can

be amplified and spread through online platforms, leading to increased levels of discrimination and hostility towards members of minority communities.

Short-term effects

Cybercrime can be a particularly traumatic experience for minority individuals, who may already feel vulnerable due to their minority status. These individuals may be more likely to experience fear and anxiety as a result of cybercrime, as they may worry about their safety both online and offline. For example, a victim of cyberstalking who is a member of a marginalized community may feel particularly threatened by the perpetrator's actions, leading to increased levels of anxiety and distress.

One of the reasons why cybercrime can be so anxiety-inducing for minority individuals is that they may feel like they are being targeted specifically because of their identity. For example, a person who is a member of an ethnic or religious minority may worry that they are being targeted by a hate group or other extremist organization. These fears can lead to a sense of isolation and helplessness, making it difficult for victims to seek the support and resources they need to recover from the crime.

Another factor that can contribute to fear and anxiety in victims of cybercrime is the uncertainty that comes with these types of crimes. Unlike physical crimes, which often leave visible evidence, cybercrimes can be difficult to detect and investigate. This can leave victims feeling like they are in a state of limbo, unsure if and when the perpetrator will strike again. The constant sense of uncertainty can be exhausting and contribute to a feeling of helplessness that can exacerbate feelings of anxiety and fear.

For minority individuals, the fear and anxiety associated with cybercrime can be compounded by the fact that they may not have access to the same resources and support as other victims. This can be due to a variety of factors, including language barriers, limited financial resources, and a lack of awareness about available resources. These barriers can make it more difficult for victims to report the crime, seek help, and recover from the trauma of the experience.

In addition to the psychological impact of cybercrime, victims may also experience tangible consequences such as financial losses, identity theft, and damage to their reputation. These consequences can be particularly devastating for minority

individuals, who may already be struggling to overcome systemic barriers to financial and social stability. The added burden of recovering from a cybercrime can make it even harder for these individuals to regain their footing and move forward with their lives.

Despite these challenges, it is important for victims of cybercrime to know that they are not alone. There are many resources available to help individuals recover from the trauma of cybercrime, including counseling services, legal assistance, and victim advocacy programs. These resources can help victims address the emotional and practical challenges of recovery, and provide them with the support they need to move forward.

In conclusion, cybercrime can be a deeply traumatic experience for minority individuals, who may already be struggling with feelings of vulnerability and marginalization. The fear and anxiety associated with cybercrime can be overwhelming, leading to a sense of isolation and helplessness. However, it is important for victims to know that there are resources available to help them recover from the trauma of cybercrime, and that they do not have to face these challenges alone. With the right support and resources, victims can overcome the psychological and practical challenges of recovery and move forward with their lives.

Cybercrime can have a profound impact on an individual's trust in technology, law enforcement, and society as a whole. For minority individuals, this loss of trust can be especially devastating, as it may reinforce feelings of marginalization and discrimination. Victims of cybercrime may feel that their concerns are not being taken seriously or that they are being unfairly targeted, further eroding their trust in these institutions.

One of the reasons why cybercrime can lead to a loss of trust is that it can be difficult to determine who is responsible for preventing and addressing these types of crimes. Technology companies, law enforcement agencies, and government organizations all play a role in addressing cybercrime, but victims may feel that these institutions are not doing enough to protect them. This can lead to a sense of frustration and disillusionment that can be difficult to overcome.

For minority individuals, the loss of trust that comes with cybercrime can be compounded by a sense of distrust and marginalization that may already exist. For example, a victim of online harassment who is a member of a marginalized community may feel that their concerns are not being taken seriously by law

enforcement because of their identity. This can lead to a sense of disillusionment and a loss of trust in law enforcement and society as a whole.

Another factor that can contribute to a loss of trust is the fact that cybercrime can be difficult to detect and prosecute. Victims may feel that there is little they can do to hold perpetrators accountable, leading to a sense of powerlessness and frustration. This can be particularly true for minority individuals, who may face additional barriers to accessing legal and law enforcement resources.

In addition to the psychological impact of a loss of trust, cybercrime can also have tangible consequences for victims. For example, a victim of identity theft may find it difficult to trust financial institutions or online vendors in the future. This can lead to a sense of isolation and a reluctance to engage with technology, further exacerbating the sense of loss and disillusionment that may already exist.

Despite these challenges, it is important for victims of cybercrime to know that there are resources available to help them rebuild their trust and regain a sense of control. Victim advocacy organizations can provide emotional support and practical resources to help victims navigate the aftermath of cybercrime. In addition, education and awareness campaigns can help to promote a better understanding of the risks and challenges associated with cybercrime, helping to restore trust in technology and society.

In conclusion, cybercrime can result in a loss of trust in technology, law enforcement, and society as a whole. For minority individuals, this loss of trust can be especially devastating, as it may reinforce feelings of marginalization and discrimination. However, with the right resources and support, victims of cybercrime can regain a sense of control and rebuild their trust in technology and society. It is important for institutions and organizations to take the concerns of victims seriously and to work to address the root causes of cybercrime, helping to restore trust and promote a safer, more equitable online environment.

Cybercrime can have severe and long-lasting consequences on the mental health of victims. For some individuals, the trauma associated with cybercrime can lead to the development of post-traumatic stress disorder (PTSD). PTSD is a condition that can develop after experiencing or witnessing a traumatic event, and it can cause symptoms such as flashbacks, nightmares, and avoidance behaviors.

In the case of cybercrime, victims may experience traumatic events such as identity theft, online harassment, or cyberstalking. These experiences can be particularly distressing because they can occur in the victim's own home, which is typically considered a safe space. Furthermore, cybercrime can be ongoing, with victims experiencing harassment or threats over a prolonged period of time, which can exacerbate the trauma.

Symptoms of PTSD can be particularly challenging to manage, and they can interfere with an individual's ability to function in daily life. For example, a victim of cyberstalking may avoid using the internet or engaging in social media to prevent further harassment, which can lead to feelings of social isolation and loneliness. Flashbacks and nightmares can also disrupt sleep and lead to difficulties with concentration and memory.

For minority individuals, the experience of cybercrime can be compounded by existing systemic inequalities and marginalization. Victims who belong to marginalized communities may experience additional stressors such as discrimination, which can further exacerbate the trauma associated with cybercrime. This can make it even more challenging to manage symptoms of PTSD and to access the support and resources needed to recover.

It is important for victims of cybercrime to seek professional help if they experience symptoms of PTSD. Mental health professionals can provide support and guidance on managing symptoms, and they can offer evidence-based treatments such as cognitive-behavioral therapy or eye movement desensitization and reprocessing (EMDR). In addition, support groups or victim advocacy organizations can provide a sense of community and understanding, which can be particularly valuable for individuals who feel isolated or marginalized.

Preventing cybercrime and addressing its root causes can also help to reduce the risk of PTSD among victims. By promoting a safer and more equitable online environment, victims may feel less vulnerable to harassment or threats, which can help to mitigate the trauma associated with cybercrime. Education and awareness campaigns can also help to reduce the stigma associated with mental health conditions such as PTSD, making it easier for victims to seek the support and resources they need.

In conclusion, cybercrime can have severe and long-lasting consequences on the mental health of victims. For some individuals, the trauma associated with

cybercrime can lead to the development of post-traumatic stress disorder (PTSD). It is important for victims to seek professional help if they experience symptoms of PTSD, and for institutions and organizations to work to prevent cybercrime and address its root causes. By promoting a safer and more equitable online environment, we can help to reduce the risk of PTSD among victims and promote a healthier, more resilient society.

Long-term effects

Chronic stress is a state of prolonged stress that can have significant negative effects on an individual's physical and mental health. For minority individuals who have experienced cybercrime, chronic stress may be an ongoing issue, leading to a range of health problems. Cybercrime can cause chronic stress due to the ongoing fear and anxiety associated with being targeted, as well as the potential loss of trust in technology, law enforcement, and society.

Chronic stress can cause a range of physical health problems, including high blood pressure, heart disease, and digestive issues. For minority individuals who may already be at higher risk of these health problems due to systemic inequalities, chronic stress associated with cybercrime can exacerbate these issues. Chronic stress can also weaken the immune system, making it more difficult to fight off infections and illnesses.

In addition to physical health problems, chronic stress can also lead to mental health issues such as depression and anxiety. The ongoing fear and anxiety associated with being targeted by cybercrime can cause significant psychological distress, leading to symptoms such as insomnia, irritability, and difficulty concentrating. Chronic stress can also interfere with an individual's ability to engage in daily activities and maintain social relationships.

For minority individuals, chronic stress associated with cybercrime can be compounded by existing systemic inequalities and marginalization. Victims who belong to marginalized communities may experience additional stressors such as discrimination, which can further exacerbate the chronic stress associated with cybercrime. This can make it even more challenging to manage physical and mental health issues associated with chronic stress.

To manage chronic stress associated with cybercrime, it is important for victims to engage in self-care practices such as exercise, healthy eating, and stress-reducing activities such as meditation or yoga. Seeking professional help from a mental health provider can also be valuable in managing chronic stress and addressing any associated physical or mental health issues. Victim advocacy organizations and support groups can also provide a sense of community and understanding, which can be particularly valuable for individuals who feel isolated or marginalized.

Preventing cybercrime and addressing its root causes can also help to reduce the risk of chronic stress among victims. By promoting a safer and more equitable online environment, victims may feel less vulnerable to harassment or threats, which can help to mitigate the chronic stress associated with cybercrime. Education and awareness campaigns can also help to reduce the stigma associated with mental health conditions and promote a more supportive and understanding society.

In conclusion, cybercrime can cause chronic stress in minority individuals, leading to a range of physical and mental health problems. It is important for victims to engage in self-care practices and seek professional help to manage chronic stress and associated health issues. Preventing cybercrime and addressing its root causes can also help to reduce the risk of chronic stress among victims and promote a healthier, more resilient society.

Cybercrime can have a significant impact on an individual's mental health, particularly in individuals who have experienced multiple incidents or have a history of mental health problems. Depression and anxiety are two of the most common mental health conditions associated with cybercrime, and they can significantly impair an individual's quality of life.

Depression is a mood disorder characterized by persistent feelings of sadness, hopelessness, and worthlessness. Cybercrime can trigger or exacerbate these feelings, particularly if the victim feels vulnerable or helpless. Victims may experience feelings of isolation, guilt, and shame, which can further contribute to depression. The loss of trust in technology, law enforcement, and society can also make it difficult for victims to seek help or support.

Anxiety is a condition characterized by excessive worry and fear about future events or situations. Cybercrime can increase the risk of anxiety, particularly if the victim feels that their safety is threatened. Victims may experience ongoing fear and worry about being targeted again, which can lead to avoidant behaviors and interfere with

their ability to engage in daily activities. The fear of being stigmatized or blamed for their victimization can also contribute to anxiety.

For individuals who have a history of mental health problems, cybercrime can further exacerbate these conditions. Victims may experience more severe symptoms or require additional treatment to manage their mental health. The ongoing fear and anxiety associated with being targeted by cybercrime can also make it more difficult for individuals to recover from their mental health problems.

To manage depression and anxiety associated with cybercrime, victims should seek professional help from a mental health provider. Therapy can be an effective way to learn coping skills and strategies to manage symptoms, as well as address any underlying mental health problems. Self-care practices such as exercise, healthy eating, and stress-reducing activities can also be helpful in managing symptoms.

Preventing cybercrime and addressing its root causes can also help to reduce the risk of depression and anxiety among victims. By promoting a safer online environment and supporting victims, society can reduce the stigma associated with mental health conditions and promote a more supportive and understanding society.

In conclusion, cybercrime can increase the risk of depression and anxiety, particularly in individuals who have experienced multiple incidents or have a history of mental health problems. Victims should seek professional help and engage in self-care practices to manage symptoms.

Social isolation is a common consequence of cybercrime, particularly if the victim feels embarrassed or ashamed about the incident. Victims may feel that others will judge them or blame them for their victimization, leading to a sense of shame and self-blame. This can make it difficult for victims to reach out for support, and they may avoid social situations altogether.

Cybercrime can also lead to a loss of trust in others and a reluctance to engage with others online or offline. Victims may feel that they cannot trust anyone, even those closest to them, leading to a sense of isolation and loneliness. This can have a significant impact on an individual's mental health, leading to symptoms of depression and anxiety.

For minority individuals, social isolation can be particularly challenging, as they may already feel disconnected from their community or society as a whole.

Cybercrime can exacerbate these feelings of disconnection and lead to a further sense of alienation. Victims may feel that they are the only ones who have experienced cybercrime, leading to a sense of isolation and loneliness.

To combat social isolation, victims should reach out to supportive friends and family members, or seek professional help from a mental health provider. Support groups and online communities can also be helpful in providing a sense of connection and understanding. Self-care practices such as exercise, healthy eating, and stress-reducing activities can also be helpful in managing symptoms and promoting a sense of well-being.

Society can also play a role in reducing social isolation among victims of cybercrime. By promoting a culture of support and understanding, society can reduce the stigma associated with victimization and provide a more welcoming environment for victims to seek help and support. Law enforcement and other authorities can also work to address the root causes of cybercrime, including improving cybersecurity measures and addressing the societal factors that contribute to victimization.

In conclusion, cybercrime can lead to social isolation, particularly if the victim feels embarrassed or ashamed about the incident. Victims should seek support from friends, family, and mental health professionals to combat feelings of loneliness and isolation. Society can also play a role in reducing social isolation by promoting a culture of support and understanding and addressing the root causes of cybercrime.

Cybercrime can have a devastating impact on an individual's finances, particularly for those who may not have the resources to recover from financial losses. Victims of cybercrime may have their bank accounts emptied, credit cards maxed out, or personal information stolen and sold on the dark web. These financial losses can have a significant impact on an individual's quality of life, leading to stress, anxiety, and even depression.

For minority individuals who may already be facing financial difficulties, the impact of cybercrime can be particularly devastating. The financial losses may further exacerbate existing financial difficulties, leading to a sense of hopelessness and desperation. Victims may also feel that they cannot seek help from law enforcement or financial institutions due to a lack of trust in these institutions or fear of further victimization.

The financial impacts of cybercrime can also have long-term consequences. Victims may have difficulty securing loans, mortgages, or credit in the future, as their credit score may be negatively impacted by the cybercrime. They may also have to spend significant time and resources trying to recover their stolen funds or identities, leading to a loss of time and productivity.

To address the financial impacts of cybercrime, victims should contact their financial institution immediately to report the incident and take steps to protect their accounts. Victims may also need to work with credit reporting agencies to ensure that their credit score is not negatively impacted by the cybercrime. In some cases, victims may be able to recover some or all of their financial losses through insurance or other forms of compensation.

Society can also play a role in addressing the financial impacts of cybercrime. Financial institutions and law enforcement agencies can work to improve cybersecurity measures and provide support and resources to victims of cybercrime. Governments can also create programs and initiatives to support victims of cybercrime, particularly those who may not have the resources to recover from financial losses on their own.

In conclusion, cybercrime can have significant financial impacts on individuals, particularly those who may not have the resources to recover from financial losses. Victims of cybercrime may experience stress, anxiety, and depression as a result of these financial losses. To address these impacts, victims should seek help from their financial institution and credit reporting agencies, and society can work to improve cybersecurity measures and provide support and resources to victims of cybercrime.

Conclusion

In order to combat cybercrime, governments and organizations around the world have developed a variety of strategies and tools. These include laws and regulations that criminalize cybercrime, as well as technological solutions such as firewalls and encryption. However, cybercrime remains a serious threat, and new types of cyberattacks are constantly emerging. As technology continues to evolve and become more integrated into our daily lives, it is likely that cybercrime will continue to be a significant challenge for law enforcement and cybersecurity professionals.

One of the key challenges in combating cybercrime is the global nature of the internet. Criminals can operate from anywhere in the world, making it difficult for law enforcement to track down and prosecute perpetrators. Additionally, the

anonymous nature of many online activities can make it difficult to identify those responsible for cybercrimes.

To address these challenges, many countries have developed international agreements and partnerships aimed at combating cybercrime. For example, the Council of Europe's Convention on Cybercrime is an international treaty that seeks to harmonize cybercrime laws and improve international cooperation in investigating and prosecuting cybercrimes. Similarly, the United States has developed partnerships with other countries to improve information sharing and coordinate efforts to combat cybercrime.

Another important tool in combating cybercrime is education and awareness. Many cybercrimes are the result of simple human error, such as falling for a phishing scam or using a weak password. By educating people about the risks of cybercrime and how to protect themselves online, we can reduce the likelihood of falling victim to these types of attacks.

Organizations can also take steps to protect themselves from cybercrime. This includes implementing strong security protocols, such as firewalls, antivirus software, and encryption. Regularly backing up data can also help mitigate the impact of a ransomware attack, as it allows organizations to restore their data without paying the ransom.

Finally, it is important to recognize that cybercrime is not just a technical problem, but also a social and economic one. Many cybercrimes are motivated by financial gain, and addressing the root causes of poverty and inequality can help reduce the incidence of cybercrime. Similarly, addressing issues such as online harassment and bullying requires a societal response, including education, awareness, and support for victims.

In conclusion, cybercrime is a growing threat that requires a multifaceted response. By developing strong partnerships between governments, organizations, and individuals, we can work together to combat cybercrime and protect ourselves from its impacts. This requires ongoing education and awareness, as well as a commitment to developing and implementing effective technological and legal solutions. As technology continues to evolve, it is likely that cybercrime will continue to be a significant challenge, but by working together we can reduce its impact and create a safer online environment for everyone.

The psychological effects of cybercrime on minority individuals can be long-lasting and traumatic. It is crucial to provide supportive services to these victims to help them cope with the emotional toll of the crime. Counseling and therapy can help

individuals process their experiences and develop strategies to cope with the stress, anxiety, and trauma that often accompany cybercrime victimization. Community support, such as support groups, can also provide a safe space for victims to connect with others who have had similar experiences and find comfort in shared understanding.

Preventing cybercrime is another critical step in addressing the psychological effects of cybercrime on minority individuals. This can include improving cybersecurity measures, raising awareness about the risks of cybercrime, and providing education and resources to help individuals protect themselves online. It is also essential to hold perpetrators accountable for their actions through the legal system to provide a sense of justice and closure to victims.

Law enforcement agencies can play a significant role in preventing cybercrime and providing justice to victims. They can work to investigate and prosecute cybercriminals, provide resources and support to victims, and raise awareness about the risks of cybercrime. However, it is also essential to address the systemic issues that may contribute to the vulnerability of minority individuals to cybercrime, such as social and economic inequality, discrimination, and lack of access to resources and education.

In addition to legal and law enforcement measures, community-based initiatives can also play a crucial role in preventing cybercrime and supporting victims. These initiatives can include education programs, community watch groups, and other outreach efforts to raise awareness about the risks of cybercrime and provide resources and support to victims.

It is essential to address the psychological effects of cybercrime on minority individuals through supportive services such as counseling, therapy, and community support. Preventing cybercrime and providing justice to victims are also critical steps in addressing the emotional toll of cybercrime victimization. Law enforcement agencies, community-based initiatives, and individuals can all play a role in preventing cybercrime and supporting victims.

References

1. Wall, D. Cybercrime: The transformation of crime in the information age. (2007).
2. Shinder, D. L. & Cross, M. Scene of the Cybercrime. (2008).
3. Lange, A. C., Duran, A. & Jackson, R. The state of LGBT and queer research in higher education revisited: Current academic houses and future possibilities. *Journal of College Student* (2019).
4. Gegenfurtner, A. & Gebhardt, M. Sexuality education including lesbian, gay, bisexual, and transgender (LGBT) issues in schools. *Educational Research Review* **22**, 215–222 (2017).
5. Chan, A. S. W., Ho, J. M. C. & Tang, P. M. K. Cancer and the LGBT Community. *J. Homosex.* **70**, 989–992 (2023).
6. Graves, K. LGBTQ education research in historical context. *LGBTQ issues in education: Advancing a research agenda* 23–42 (2015).
7. Marcum, C. D. & Higgins, G. E. Cybercrime. (2019).

8. Prasanthi, B. V. & Kanakam, P. Cyber forensic science to diagnose digital crimes-a study. *International Journal of* (2017).

9. Gayed, T. F., Lounis, H. & Bari, M. Cyber forensics: Representing and (im) proving the chain of custody using the semantic web. in *COGNITIVE 2012: The Fourth International Conference on Advanced Cognitive Technologies and Applications* 19–23 (Citeseer, 2012).

10. Mnyakin, M. Investigating the Impacts of AR, AI, and Website Optimization on Ecommerce Sales Growth. *RRST* **3**, 116–130 (2020).

11. Karat, C. M., Blom, J. O. & Karat, J. *Designing personalized user experiences in eCommerce*. (Springer, 2004).

12. Jaishankar, K. Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology* (2007).

13. Telo, J. ANALYZING THE EFFECTIVENESS OF BEHAVIORAL BIOMETRICS IN AUTHENTICATION: A COMPREHENSIVE REVIEW. *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries* **2**, 19–36 (2019).

14. Nowaskie, D. Z. & Patel, A. U. How much is needed? Patient exposure and curricular education on medical students' LGBT cultural competency. *BMC Med. Educ.* **20**, 490 (2020).

15. Bonvicini, K. A. LGBT healthcare disparities: What progress have we made? *Patient Educ. Couns.* (2017).
16. Daley, A. & MacDonnell, J. A. “That would have been beneficial”: LGBTQ education for home-care service providers. *Health Soc. Care Community* (2015).
17. Matza, A. R., Sloan, C. A. & Kauth, M. R. Quality LGBT health education: A review of key reports and webinars. *Parent. Sci. Pract.* (2015).
18. Chan, A. S. K. & Ho, W. C. “My community doesn’t belong to me anymore!”: Tourism-driven spatial change and radicalized identity politics in Hong Kong. *Living in the Margins in Mainland China* (2020).
19. Renn, K. A. LGBT and Queer Research in Higher Education: The State and Status of the Field. *Educ. Res.* **39**, 132–141 (2010).
20. Bilodeau, B. L. & Renn, K. A. Analysis of LGBT identity development models and implications for practice. *New Dir. Stud. Serv.* **2005**, 25–39 (2005).
21. Carabez, R., Pellegrini, M., Mankovitz, A. & Eliason, M. “Never in all my years…”: Nurses’ education about LGBT health. *Journal of Professional* (2015).
22. Chan, A. S. K. The Production of Estranged Urban Space: Tourism--driven Community Change and Radicalised Identity Politics in Hong Kong Since the 2010s. (City University of Hong Kong, 2020).

23. Harichandran, V. S., Breitinger, F., Baggili, I. & Marrington, A. A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Comput. Secur.* **57**, 1–13 (2016).

24. Telo, J. Understanding Security Awareness Among Bank Customers: A Study Using Multiple Regression Analysis. *Sage Science Review of Educational Technology* **6**, 26–38 (2023).

25. Marcella, A., Jr & Menendez, D. Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes. (2010).

26. Baggili, I. & Breitinger, F. Data sources for advancing cyber forensics: What the social world has to offer. https://cdn.aaai.org/ocs/10227/10227-45279-1-PB.pdf (2015).

27. Shrivastava, G., Sharma, K., Khari, M. & Zohora, S. E. Role of Cyber Security and Cyber Forensics in India. in *Handbook of Research on Network Forensics and Analysis Techniques* 143–161 (IGI Global, 2018).

28. Harman, R. Continuing conversations: A review ofLGBTQ Youth and Education: Policies and Practices. *J. LGBT Youth* **14**, 122–127 (2017).

29. Chan, A. S. W., Ho, J. M. C., Li, J. S. F. & Tam, H. L. Impacts of COVID-19 pandemic on psychological well-being of older chronic kidney disease patients. *Frontiers in Medicine* (2021).

30. Jones, T. Education policies: Potential impacts and implications in Australia and beyond. *J. LGBT Youth* **13**, 141–160 (2016).

31. Nardi, H. C. Theoretical approaches and policies in sexual diversity and educational in Brazil: A critical review. *J. LGBT Youth* **8**, 201–209 (2011).

32. Brinson, A., Robinson, A. & Rogers, M. A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital Investigation* **3**, 37–43 (2006).

33. Telo, J. A Comparative Analysis of Network Security Technologies for Small and Large Enterprises. *International Journal of Business Intelligence and Big Data Analytics* **2**, 1–10 (2019).

34. Park, H., Cho, S. & Kwon, H.-C. Cyber Forensics Ontology for Cyber Criminal Investigation. in *Forensics in Telecommunications, Information and Multimedia* 160–165 (Springer Berlin Heidelberg, 2009).

35. Prasanthi, B. V. & Vishnu Institute of Technology. Cyber Forensic Tools: A Review. *Int. J. Eng. Trends Technol.* **41**, 266–271 (2016).

36. Telo, J. Blockchain Technology in Healthcare: A Review of Applications and Implications. *Journal of Advanced Analytics in Healthcare Management* **1**, 1–20 (2017).

37. McConnell, E. A., Birkett, M. A. & Mustanski, B. Typologies of Social Support and Associations with Mental Health Outcomes Among LGBT Youth. *LGBT Health* **2**, 55–61 (2015).

38. Eliason, M. J., Dibble, S. L. & Robertson, P. A. Lesbian, gay, bisexual, and transgender (LGBT) physicians' experiences in the workplace. *J. Homosex.* **58**, 1355–1371 (2011).

39. Sekoni, A. O., Gale, N. K., Manga-Atangana, B., Bhadhuri, A. & Jolly, K. The effects of educational curricula and training on LGBT-specific health issues for healthcare students and professionals: a mixed-method systematic review. *J. Int. AIDS Soc.* **20**, 21624 (2017).

40. Chan, A. S. W. *et al.* Impacts of psychological wellbeing with HIV/AIDS and cancer among sexual and gender minorities: A systematic review and meta-analysis. *Front Public Health* **10**, 912980 (2022).

41. Cahill, S. & Makadon, H. Sexual Orientation and Gender Identity Data Collection in Clinical Settings and in Electronic Health Records: A Key to Ending LGBT Health Disparities. *LGBT Health* **1**, 34–41 (2014).

42. Ryan, C., Russell, S. T., Huebner, D., Diaz, R. & Sanchez, J. Family acceptance in adolescence and the health of LGBT young adults. *J. Child Adolesc. Psychiatr. Nurs.* **23**, 205–213 (2010).

43. Balsam, K. F., Molina, Y., Beadnell, B., Simoni, J. & Walters, K. Measuring multiple minority stress: the LGBT People of Color Microaggressions Scale. *Cultur. Divers. Ethnic Minor. Psychol.* **17**, 163–174 (2011).

44. Chan, A. S. W., CPsychol, RSWPhD. Letter to the Editor: Advocating Worldwide Social Inclusion and Anti-Discrimination Among LGBT Community. *J. Homosex.* **70**, 779–781 (2023).

45. Gordon, S. & Ford, R. On the definition and classification of cybercrime. *Journal in computer virology* (2006).

46. Cho, C., Chin, S. & Chung, K. S. Cyber forensic for hadoop based cloud system. *International Journal of Security and its Applications* **6**, 83–90 (2012).

47. Luciano, L., Baggili, I., Topor, M., Casey, P. & Breitinger, F. Digital Forensics in the Next Five Years. in *Proceedings of the 13th International Conference on Availability, Reliability and Security* 1–14 (Association for Computing Machinery, 2018).

48. Telo, J. Web Traffic Prediction Using Autoregressive, LSTM, and XGBoost Time Series Models. *Web Traffic Prediction Using Autoregressive, LSTM, and XGBoost Time Series Models* **3**, 1–15 (2020).

49. Marcella, A. J. & Guillossou, F. *Cyber forensics: From data to digital evidence*. (John Wiley & Sons, 2012).

50. Telo, J. Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. *International Journal of Intelligent Automation and Computing* **6**, 31–45 (2023).

51. Walsh, D. & Hendrickson, S. G. Focusing on the "T" in LGBT: An online survey of related content in Texas nursing programs. *J. Nurs. Educ.* (2015).

52. Sequeira, G. M., Chakraborti, C. & Panunti, B. A. Integrating Lesbian, Gay, Bisexual, and Transgender (LGBT) Content Into Undergraduate Medical School Curricula: A Qualitative Study. *Ochsner J.* **12**, 379–382 (2012).

53. Sintos Coloma, R. Ladlad and Parrhesiastic Pedagogy: Unfurling LGBT Politics and Education in the Global South. *Curriculum Inquiry* (2013).

54. Chan, A. S. W. Book Review: Safe Is Not Enough: Better Schools for LGBTQ Students (Youth Development and Education Series). (2021).

55. Nowaskie, D. A national survey of U.S. psychiatry residents' LGBT cultural competency: The importance of LGBT patient exposure and formal education. *J. Gay Lesbian Ment. Health* **24**, 375–391 (2020).

56. Flores, G. Toward a More Inclusive Multicultural Education: Methods for Including LGBT Themes in K-12 Classrooms. *Am. J. Sex. Educ.* **7**, 187–197 (2012).

57. Mayo, C. & Banks, J. A. *LGBTQ youth and education: Policies and practices*. (Teachers' College Press, 2022).

58. Chan, A. S. W. & Tang, P. M. K. Application of Novel Psychoactive Substances: Chemsex and HIV/AIDS Policies Among Men Who Have Sex With Men in Hong Kong. *Front. Psychiatry* **12**, 680252 (2021).

59. Dardick, G. S. Cyber Forensics Assurance. (2010) doi:10.4225/75/57b2926c40cda.

60. Telo, J. Intrusion Detection with Supervised Machine Learning using SMOTE for Imbalanced Datasets. *Journal of Artificial Intelligence and Machine Learning in Management* **5**, 12–24 (2021).

61. Santanam, R., Sethumadhavan, M. & Virendra, M. *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives*. (Information Science Reference, 2010).

62. Kotenko, I. V., Kolomeets, M., Chechulin, A. & Chevalier, Y. A visual analytics approach for the cyber forensics based on different views of the network traffic. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.* **9**, 57–73 (2018).

63. Patil, R. Y. & Devane, S. R. Unmasking of source identity, a step beyond in cyber forensic. in *Proceedings of the 10th International Conference on Security of Information and Networks* 157–164 (Association for Computing Machinery, 2017).

64. Telo, J. AI for Enhanced Healthcare Security: An Investigation of Anomaly Detection, Predictive Analytics, Access Control, Threat Intelligence, and Incident Response. *Journal of Advanced Analytics in Healthcare Management* **1**, 21–37 (2017).

65. Martin, J. I., Messinger, L., Kull, R. & Holmes, J. Council on Social Work Education–Lambda legal study of LGBT issues in social work. *Soc. Work Educ.* (2009).

66. Chan, A. S. W. Book review: the Educator's guide to LGBT+ inclusion: a practical resource for K-12 teachers, administrators, and school support staff. (2021).

67. Meyer, E. J. The personal is political: LGBTQ education research and policy since 1993. *Educ. Forum* (2015).

68. Taylor, C. G., Meyer, E. J., Peter, T. & Ristock, J. Gaps between beliefs, perceptions, and practices: The Every Teacher Project on LGBTQ-inclusive education in Canadian schools. *Journal of LGBT* (2016).

69. Aragon, S. R., Poteat, V. P. & Espelage, D. L. The influence of peer victimization on educational outcomes for LGBTQ and non-LGBTQ high school students. *Journal of LGBT* (2014).

70. Hardacker, C. T., Rubinstein, B. & Hotton, A. Adding silver to the rainbow: the development of the nurses' health education about LGBT elders (HEALE) cultural competency curriculum. *Journal of Nursing* (2014).

71. Hirschtritt, M. E., Noy, G., Haller, E. & Forstein, M. LGBT-Specific Education in General Psychiatry Residency Programs: a Survey of Program Directors. *Acad. Psychiatry* **43**, 41–45 (2019).

72. Chan, A. S. W., Li, J. S. F., Ho, J. M. C., Tam, H. L. & Hsu, W. L. The systematic review and meta-analysis of Chronic Inflammation and Fibrosis in HIV/AIDS and Cancer: Impacts of Psychological Wellbeing among …. *Frontiers in Public*.

73. McQuade, S. C. Understanding and managing cybercrime. (2006).

74. Cech, E. A. & Rothwell, W. R. LGBTQ inequality in engineering education. *J. Eng. Educ.* **107**, 583–610 (2018).

75. Chan, A. S. W. Book review: the deviant's war: the homosexual vs. the United States of America. (2021).

76. Kull, R. M., Kosciw, J. G. & Greytak, E. A. Preparing School Counselors to Support LGBT Youth: The Roles of Graduate Education and Professional Development. *Professional School Counseling* **20**, 1096-2409–20.1a.13 (2017).

77. Cooper, M. B., Chacko, M. & Christner, J. Incorporating LGBT Health in an Undergraduate Medical Education Curriculum Through the Construct of Social Determinants of Health. *MedEdPORTAL* **14**, 10781 (2018).

78. Allen, L. Queering the academy: new directions in LGBT research in higher education. *Higher Education Research & Development* **34**, 681–684 (2015).

79. Keuroghlian, A. S., Ard, K. L. & Makadon, H. J. Advancing health equity for lesbian, gay, bisexual and transgender (LGBT) people through sexual health education and LGBT-affirming health care environments. *Sex. Health* **14**, 119–122 (2017).

80. Russell, S. T. & Fish, J. N. Mental Health in Lesbian, Gay, Bisexual, and Transgender (LGBT) Youth. *Annu. Rev. Clin. Psychol.* **12**, 465–487 (2016).

81. Almeida, J., Johnson, R. M., Corliss, H. L., Molnar, B. E. & Azrael, D. Emotional distress among LGBT youth: the influence of perceived discrimination based on sexual orientation. *J. Youth Adolesc.* **38**, 1001–1014 (2009).

82. Chan, A. S. W., Tang, P. M. K. & Yan, E. Chemsex and its risk factors associated with human immunodeficiency virus among men who have sex with men in Hong Kong. *World Journal of Virology* (2022).

83. Meyer, I. H. Minority stress and positive psychology: Convergences and divergences to understanding LGBT health. *Psychology of Sexual Orientation and Gender Diversity* **1**, 348–349 (2014).

84. Hermosillo, D., Cygan, H. R., Lemke, S., McIntosh, E. & Vail, M. Achieving health equity for LGBTQ+ adolescents. *J. Contin. Educ. Nurs.* **53**, 348–354 (2022).

85. Catalano, D. C. J. The paradoxes of social justice education: Experiences of LGBTQ+ social justice educational intervention facilitators. *J. Divers. High. Educ.* (2022) doi:10.1037/dhe0000436.

86. Chan, A. S. W., Ho, J. M. C., Tam, H. L., Hsu, W. L. & Tang, P. M. K. COVID-19, SARS, and MERS: the risk factor associated with depression and its impact on psychological well-being among sexual moralities. (2022).

87. Cornelius, E. & Fabro, M. *Recommended practice: Creating cyber forensics plans for control systems*. https://www.osti.gov/biblio/944209 (2008) doi:10.2172/944209.

88. Telo, J. Supervised Machine Learning for Detecting Malicious URLs: An Evaluation of Different Models. *Sage Science Review of Applied Machine Learning* **5**, 30–46 (2022).

89. Stirland, J., Jones, K., Janicke, H., Wu, T. & Others. Developing cyber forensics for SCADA industrial control systems. in *Proceedings of the International*

Conference on Information Security and Cyber Forensics (Universiti Sultan Zainal Abidin Kuala Terengganu, Malaysia, 2014).

90. Nirkhi, S. & Dharaskar, R. V. Comparative study of Authorship Identification Techniques for Cyber Forensics Analysis. *arXiv [cs.CY]* (2013).
91. Anderson, R. *et al.* Measuring the Cost of Cybercrime. in *The Economics of Information Security and Privacy* (ed. Böhme, R.) 265–300 (Springer Berlin Heidelberg, 2013).
92. Göçmen, İ. & Yılmaz, V. Exploring Perceived Discrimination Among LGBT Individuals in Turkey in Education, Employment, and Health Care: Results of an Online Survey. *J. Homosex.* **64**, 1052–1068 (2017).
93. Chan, A. S. W., Ho, J. M. C., Tam, H. L. & Tang, P. M. K. Book review: successful aging: a neuroscientist explores the power and potential of our lives. *Front. Psychol.* (2021).
94. Navarro, M. A., Hoffman, L., Crankshaw, E. C., Guillory, J. & Jacobs, S. LGBT Identity and Its Influence on Perceived Effectiveness of Advertisements from a LGBT Tobacco Public Education Campaign. *J. Health Commun.* **24**, 469–481 (2019).
95. McNiel, P. L. & Elertson, K. M. Advocacy and Awareness: Integrating LGBTQ Health Education Into the Prelicensure Curriculum. *J. Nurs. Educ.* **57**, 312–314 (2018).

96. Korolczuk, E. The fight against 'gender'and "LGBT ideology": new developments in Poland. *European journal of politics and gender* (2020).

97. Chan, A. S. W., Wu, D., Lo, I. P. Y., Ho, J. M. C. & Yan, E. Diversity and Inclusion: Impacts on Psychological Wellbeing Among Lesbian, Gay, Bisexual, Transgender, and Queer Communities. *Front. Psychol.* **13**, 726343 (2022).

98. Eickhoff, C. Identifying Gaps in LGBTQ Health Education in Baccalaureate Undergraduate Nursing Programs. *J. Nurs. Educ.* **60**, 552–558 (2021).

99. Baams, L., Dubas, J. S. & van Aken, M. A. G. Comprehensive Sexuality Education as a Longitudinal Predictor of LGBTQ Name-Calling and Perceived Willingness to Intervene in School. *J. Youth Adolesc.* **46**, 931–942 (2017).

100. Nash, C. J. & Browne, K. Resisting the mainstreaming of LGBT equalities in Canadian and British Schools: Sex education and trans school friends. *Environment and Planning C: Politics and Space* **39**, 74–93 (2021).

101. Landi, D. LGBTQ youth, physical education, and sexuality education: Affect, curriculum, and (new) materialism. (2019).

102. Chan, A. S. W., Lo, I. P. Y. & Yan, E. Health and Social Inclusion: The Impact of Psychological Well-Being and Suicide Attempts Among Older Men Who Have Sex With Men. *Am. J. Mens. Health* **16**, 15579883221120984 (2022).

103. Utamsingh, P. D., Kenya, S., Lebron, C. N. & Carrasquillo, O. Beyond sensitivity. LGBT healthcare training in U.s. medical schools: A review of the literature. *Am. J. Sex. Educ.* **12**, 148–169 (2017).

104. Russell, S. T., Horn, S., Kosciw, J. & Saewyc, E. Safe Schools Policy for LGBTQ Students and commentaries. *Soc. Policy Rep.* **24**, 1–25 (2010).

105. Telo, J. PRIVACY AND CYBERSECURITY CONCERNS IN SMART GOVERNANCE SYSTEMS IN DEVELOPING COUNTRIES. *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries* **4**, 1–13 (2021).

106. McGlashan, H. & Fitzpatrick, K. LGBTQ youth activism and school: Challenging sexuality and gender norms. *Health Educ.* (2017).

107. Chan, A. S. W. Book review: the gay revolution: the story of the struggle. (2021).

108. Landi, D., Flory, S. B. & Safron, C. LGBTQ Research in physical education: a rising tide? *Phys. Educ. Sport Pedagogy* (2020).

109. Jacobs, J. & Freundlich, M. Achieving permanency for LGBTQ youth. *Child Welfare* **85**, 299–316 (2006).

110. Elia, J. P. & Eliason, M. J. Dangerous Omissions: Abstinence-Only-Until-Marriage School-Based Sexuality Education and the Betrayal of LGBTQ Youth. *Am. J. Sex. Educ.* **5**, 17–35 (2010).

111. Furnell, S. Cybercrime: Vandalizing the information society. (2002).

112. Holt, T. J. & Bossler, A. M. Cybercrime in progress: Theory and prevention of technology-enabled offenses. (2015).

113. Broadhurst, R. & Chang, L. Y. C. Cybercrime in Asia: Trends and Challenges. in *Handbook of Asian Criminology* (eds. Liu, J., Hebenton, B. & Jou, S.) 49–63 (Springer New York, 2013).